



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

mj

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,653	12/20/2001	James M. Vignoles	NAIIP048/01.183.01	2731
28875	7590	10/12/2006	EXAMINER	
Zilka-Kotab, PC P.O. BOX 721120 SAN JOSE, CA 95172-1120			PYZOWA, MICHAEL J	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 10/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/028,653	VIGNOLES ET AL.
Examiner	Art Unit	
Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Statyus

1) Responsive to communication(s) filed on 18 August 2006.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-5,7,11-16,18,22,23 and 28-33 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-5,7,11-16,18,22,23 and 28-33 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____
5) Notice of Informal Patent Application
6) Other: _____

DETAILED ACTION

1. Claims 1-5, 7, 11-16, 18, 22-23, 28-33 are pending.
- 2.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 12-16 and 18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 12-16 and 18 relate to a computer product with computer code stored on a tangible medium, this code is merely descriptive material because the code does not perform any action nor cause any action to be performed. Therefore claims 12-16 and 18 are held to be non-statutory.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the

Art Unit: 2137

art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-5, 7, 12-16, 18, 23, 29, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over ConSeal PC FIREWALL Technical Summary (hereinafter ConSeal) in view of Hari et al (Detecting and resolving packet filter conflicts) and in view of Coss et al (US 6098172) and further in view of Chan et al (US 6910028).

As per claims 1, 12, 23, and 29, ConSeal discloses identifying a set of policies, each policy having a condition associated therewith; determining whether the conditions are met; and activating the policies whose associated conditions are determined to be met (see pages 1-2) wherein the activation of the policies includes adding the policies to a set of a plurality of active policies, and executing security actions associated with the active policies if associated limits are met (see pages 1-2).

ConSeal fails to disclose the conditions represent different policies, which are based on priority and determining and resolving any conflicts and the conditions include a time factor, which is at least one of a timeframe, a predetermined time period, and a time limit, and the conditions include a source of the policies.

However, Hari et al teaches such policy priorities and conflict resolution (see page 1204 section II) and Coss et al teaches the use of a time factor (see column 2 lines 29-41) and Chan et al teaches the conditions include a source of the policy (see column 7 line 60 through column 8 line 33).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Hari et al's priorities, conflict resolution and the time factors of Coss et al and the source identification of Chan et al in the firewall system of ConSeal.

Motivation to do so would have been to avoid matching multiple filters with confliction actions (see Hari et al page 1204 section II) and to allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded (see Coss et al column 2 lines 29-41) and it enables deep semantic guarantees including consistency (see column 7 line 60 through column 8 line 33).

As per claims 2-3 and 13-14, the modified ConSeal, Hari et al, Coss et al, and Chan et al system discloses activating the policies if the user confirms (see ConSeal page 2).

As per claims 4-5 and 15-16, the modified ConSeal, Hari et al, Coss et al, and Chan et al system discloses updating includes receiving another inactive policy, determining whether

the user accepts the inactive policy, and adding the inactive policy to the set if the user accepts the inactive policy (see ConSeal page 2).

As per claims 7 and 18, the modified ConSeal, Hari et al, Coss et al, and Chan et al system discloses determining whether the conditions associated with the active policies are still met, and de-activating the active policies if the associated conditions are not met (see bottom of page 1 to the top of page 2).

As per claim 33, the modified ConSeal, Hari et al, Coss et al, and Chan et al system discloses the identifying, determining and activating are controlled locally (see ConSeal page 1).

6. Claims 11 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified ConSeal, Hari et al, Coss et al, and Chan et al system as applied to claims 1 and 12 above, and further in view of Porras et al (US 6704874).

As per claims 11 and 22, the modified ConSeal, Hari et al, Coss et al, and Chan et al system fails to disclose the conditions include a severity of the security actions associated with the policies.

However, Porras et al teaches such a prioritization technique (see column 2 lines 46-51 where a more severe of the attack requires a more severe action).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Porras et al's prioritization teaching in the modified ConSeal, Hari et al, Coss et al, and Chan et al system.

Motivation to do so would have been to allow for a tag to be included to relate the severity.

7. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified ConSeal, Hari et al, Coss et al, and Chan et al system as applied to claim 1 above, and further in view of Horvitz et al (US 2003021621).

As per claim 28, the modified ConSeal, Hari et al, Coss et al, and Chan et al system fails to disclose the conditions represent an urgency associated with an issue causing the policy to be activated.

However, Brock et al teaches such a priority based on urgency (see paragraph 117).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Brock et al's teaching of urgency based priority in the modified ConSeal, Hari et al, Coss et al, and Chan et al system.

Motivation to do so would have been to facilitate efficient processing of electronic information while mitigating the costs of manual interventions associated therewith (see paragraph 6).

8. Claims 30-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified ConSeal, Hari et al, Coss et al, and Chan et al system as applied to claim 1 above, and further in view of Cisco (IPSec User Guide for the Cisco Secure PIX Firewall Version 5.2).

As per claims 30-32, the modified ConSeal, Hari et al, Coss et al, and Chan et al system fails to disclose three policies with different priorities having different valid time periods.

However Cisco teaches such policies (see "Enabling and Configuring IKE" pages 6-1 and 6-2).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the policies of Cisco in the modified ConSeal, Hari et al, Coss et al, and Chan et al system.

Motivation to do so would have been to allow the firewall to use Internet Key Exchange (see top of page 6-1).

Response to Arguments

9. Applicant's arguments with respect to the newly added limitations to claims 1, 12, 23, 26 and 28 have been considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments filed 04/18/2006 have been fully considered but they are not persuasive. Applicant argues:

ConSeal fails to disclose executing security actions associated with the active policies if associated limits are met; Hari fails to teach activating policies under different priority conditions and teaches away from the claimed priority policy; Brock fails to disclose the conditions represent an urgency; Beebe fails to disclose the conditions include a source of the policies; ConSeal fails to disclose user confirmation to activate the policies; ConSeal fails to disclose receiving an inactive policy and adding it if the user accepts; Porras fails to disclose including a severity of security actions associated with the policies.

With respect to Applicant's argument that ConSeal fails to disclose executing security actions associated with the active policies if associated limits are met, each time a packet is filtered (i.e. not allowed through the firewall) that is the ConSeal firewall executing a security action associated with the active policies when a limit is met because a match in the policy corresponds to a limit.

With respect to Applicant's argument that Hari fails to teach activating policies under different priority conditions when a conflict arises the filter with the highest priority is selected and when only a single filter matches, i.e. no conflict, that filter is activated because it has the highest

Art Unit: 2137

(an only priority) which is a second priority related activation of a policy different than the first. With respect to Applicant's argument that Hari teaches away from the claimed priority policy, the priority based system of Hari teaches that each filter (i.e. policy) has a different priority and when a packet matches more than one filter, which ever filter has a higher priority is used. Therefore, Hari does not teach away from the claimed limitation of, "wherein a first policy with a higher priority has a first condition associated therewith that is different from a second condition associated with a second policy with a lower priority such that the first policy and second policy are activated under different priority related conditions".

Applicant's argument that Brock fails to disclose the conditions represent an urgency and that Beebe fails to disclose the conditions include a source of the policies are moot in view of new grounds of rejection.

With respect to Applicant's argument that ConSeal fails to disclose user confirmation to activate the policies, when a rule in ConSeal has not been used before and the system is in Checked Learning Mode, the user is prompted to make a rule for the packet (i.e. allow or disallow) thereby creating two inactive policies (one to allow the packet and one to disallow the

Art Unit: 2137

packet). Therefore when the user selects an action the user is activating one of the previous inactive rules.

With respect to Applicant's argument that ConSeal fails to disclose receiving an inactive policy and adding it if the user accepts, ConSeal allows for an administrator to make a rule remotely and a user can download this rule (as evidenced by page 4 of the Mien reference supplied on 09/21/2005). When a user chooses to download a policy (receiving a policy) it is inactive because it is not loaded or in anyway activated by the system it is merely data. When the user loads the set into the program that is the user accepting the inactive policy.

With respect to Applicant's argument that Porras fails to disclose including a severity of security actions associated with the policies, Porras teaches tagging alerts with a flag indicating the severity of the attack. These alerts are generated based on filtering conditions being met (see column 1 lines 51-62) and therefore are associated with the conditions being met and the more severe an attack the more severe the action in response to the attack will be.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Ahlstrom et al

(US 6327618) provides a system to resolve conflicts based on priorities.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Application/Control Number: 10/028,653
Art Unit: 2137

Page 12

MJP



EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER